LNPA Transition Will Take 2½ Years Following Final Approval of Selection

Phase	Minimum Duration	Tasks and Impacts
[redacted]	[redacted]	• [redacted]
Implementation	8 months	• Build and test new NPAC/SMS • Define and document all LNPA services not specified in the RFP • Configure/enhance SOAs and LSMSs to connect to new NPAC/SMS, and multiple NPAC/SMSs during regional overlap • Establish new performance monitoring and reporting • Define and certify neutrality program and other service audits
[redacted]	[redacted]	• [redacted]
Testing	8 months	• Most critical and iterative phase of transition • Multiple sequential steps: functional acceptance testing, performance and stress testing, vendor testing, Service Provider/end-to-end testing, and multiple "dry-runs" of final cut-over • Testing for all LNPA services ancillary to the NPAC/SMS
[redacted]	[redacted]	• [redacted]
TOTAL	**29 months**	• **Final cutover in July 2016 assuming start date of FCC approval of selection in January 2014**

Note: alternative vendors are likely to claim that ancillary experience—offering NPAC simulators, SOA platforms, or international LNP—constitute relevant experience in U.S. LNP administration that can compress the transition timeline. This claim should be treated with the appropriate skepticism, given the unique functional and performance profile of the U.S. NPAC/SMS.

Subscriber Impacts—Although testing is critical prior to transition, there is no substitute for time and real-world experience to deliver stability and consistent performance. It took several years for Neustar to reach today's performance level, in a substantially simpler environment than what exists today. The Industry should assume at least two years of degraded performance AFTER transition is finally complete.

The impacts to consumers and Service Providers resulting from instability will be considerable, and issues that arise during transition for one Service Provider are certain to ripple throughout the rest of the Industry. Attached to Neustar's April 5th proposal is an analysis developed by Navigant Economics that provides a comprehensive assessment of the direct costs and subscriber impacts of a transition to a new vendor. Navigant's analysis assumes 99.98% accuracy on the initial database conversion, and 99.7% accuracy on broadcast transactions in the first year, and concludes that over **7 million subscribers** will be **impacted** in the **first year** of transition due to porting delays, misrouted calls, or other service failures. This results in over **$719 million in direct costs and service credits**. If the Industry takes more than one year to restore stability to the LNPA service, these costs **rise to over $1 billion**.

In addition to the direct costs of data errors and broadcast failures, degradation in the porting experience has direct impacts on Service Provider revenue. A small percentage of porting subscribers (less than one percent in the Navigant model) will experience such severe issues in the porting experience that they will abandon their interest in switching providers. Lifetime **gross profit** for these subscribers is equivalent to **another $410 million in the first year** of transition.

Opportunity Costs—Transition to a new vendor will involve two years of planning and execution, and a further two years of instability and issue resolution, resulting in a **total of four years** (until 2018) during which the Industry will have limited capacity to focus on their strategic business priorities—including IP migrations, M&A, and revenue-generating innovation.

Cost and Risk Analysis

The analysis below shows that the transition costs and risks as previously described exceed any financial advantage gained over the next contract term from selecting an alternative vendor—even at half Neustar's Best and Final Offer. For smaller regional or multi-Service Providers, the analysis indicates that there is no competitive price that makes a transition financially attractive.

No Financial Advantage From Transition—Even at Half Neustar's BAFO

	Full Industry	Typical Regional or Multi-Service Provider
Subscribers	~400M	~7M
Telecommunications revenue	~$300B	~$5B
[redacted]		
Extended Neustar contract & transition services	[redacted]	$6M
Subscriber Impacts: Customer Care & operations	$719M	$14M
Subscriber Impacts: Customer acquisition	$410M	$8M
Total	[redacted]	**$28M**

All Reward and No Risk

- By selecting Neustar, the Industry receives the following benefits, immediately and at zero risk
  - Year-one price reductions of over [redacted]; over [redacted] in total savings from existing contract
  - Certainty of continued performance and value—underpinning billions of dollars in revenue from acquired customers and flawless network transactions
  - An experienced management team with over 420 years of experience successfully serving as the U.S. LNPA
  - A stable and secure partner in the execution of critical Industry priorities—including M&A and the migration to IP
  - Complete confidence in the LNPA's commitments to neutrality, information security, and data privacy
- By contrast, the full costs of choosing an untested alternate vendor include:
  - A high-risk and disruptive transition process, lasting at least four years and costing the Industry over $1 billion
  - Prolonged subscriber impacts resulting from instability, performance degradation, and service gaps
  - A multi-year incapacity to focus on essential Industry change
  - Unknown future compromises in neutrality and transparency

By selecting a vendor other than Neustar, the Industry will incur greater expense in contact extensions, subscriber instability, and opportunity cost each and every year until 2018. This is the case for the Industry as a whole—and for most Service Providers, given their dependency on the continued high performance of Neustar and NPAC/SMS, there is no benefit to a transition at any price.

Neustar again thanks the FoNPAC and the NAPM, LLC for its consideration in the procurement of LNPA services. We are prepared to answer any additional questions the selectors have about our offer.

Appendix A: Evaluation Criteria

The following table describes Neustar's qualifications and commitments against the RFP's Evaluation Criteria.

Criterion	How Neustar Meets/Exceeds Requirements
Factor 1: Operational Performance	• Proven levels of excellence delivering core functions today (Proposal Section 1.1): o Service and operations **are fully compliant** today with neutrality requirements o Provides over 100 monthly reports with **100% accuracy** o Issues over **11,000** invoices each month with **over 99.5%** accuracy o Resolves over 80% of Industry calls at the first tier of Customer Support o Successfully **managed and implemented over 450 NANC change orders** and well over 100 Illinois change orders o Supports Industry testing, with over **4,200 hours of support** in 2012 alone, **scoring 3.8 out of 4** in third-party audit for knowledge, responsiveness, availability, management, etc. • Value-added, proactive functions such as (Proposal Section 1.1): o Provisions customer requests (e.g., creates, activates, modifies, SPID migrations, Mass updates/port requests, NPA splits, etc) with **>99.9% accuracy**; over 55,000 MUMP requests processed in 2012 o Service Management proactively monitors entire connected ecosystem notifying SPs of slowness in their systems o Unmatched expertise and Industry knowledge provided via the npac.com website, Industry meetings, Industry notifications, and training offerings o Proactive disaster preparedness (via increased coverage, proactive notifications, enabling virtual routing, etc..) and efficient disaster recovery services that maximize Industry service delivery in times of disaster • **NEW** NPAC Portal with a consolidated interface and greater automation, robust real-time reporting, chat with an expert, e-invoicing and a market-leading Information Analytics Platform • **NEW** Enhanced testing capabilities for Industry self service/self certification • **NEW** Dedicated 24x7x365 customer support • **NEW** Enhanced suite of training modules • **Zero operational implementation** required (Proposal Section 1.6)
Factor 2: Reliability and Functionality	• Fully compliant **today** with all RFP requirements; over the last five years, **met or exceeded** Industry's 27 SLRs **99.94%** of the time (Proposal Section 1.2) • **Zero transition required** and accompanying risks/costs avoided (Proposal Section 1.6) • Customized Approach to Operational Excellence (Proposal Section 1.3) o Design, engineering, and operations teams within a single Neustar entity, in the United States, to maximize performance and accountability o Security-Related Information o Continual technical refreshes prior to identified end of life—Replaced every component of the NPAC at least twice in the last eight years • ISO-certified Disaster recovery process and successful completion of annual fail over exercise for the past 10 years (Proposal Section 1.2.4) • **NEW** Increased automation/refinements to meet new SLRs (Proposal Section 1.2.1/1.2.2) • **NEW** Additional ISO certifications—TL 9000 Quality Management System; ISO 27001—Information Security; and ISO 22301—Business Continuity (Proposal Section 1.3) • **NEW** All required enhancements stated in RFP Section 7.0 including Security-Related Information, support of IPv6, and elimination of NPAC/SMS support of Non-EDR (Proposal Sections 1.2.2, 1.5) • **NEW** Unmatched ability to implement "future considerations" detailed in RFP Section 7 with the least amount of risk and the highest levels of quality and results (Proposal Sections 1.2.2, 1.5) • **NEW** Expanded capabilities and services driving incremental value to SPs and Consumers (Proposal Section 1.5)

Criterion	How Neustar Meets/Exceeds Requirements
Factor 3: Security-Related In	Security-Related Information
[redacted]	
Factor 1: Customer Service	• Proven service-oriented, neutral approach to serving as the LNP Administrator measuring customer satisfaction via: o Third-party, Industry-wide Annual NPAC User Survey (Proposal Section 2.5) o Transactional based surveys after each interaction with the Help Desk, Customer Connectivity Services, and MUMP teams o NPAC.com real-time feedback mechanisms • Received **3.84 out of 4.00 Overall Customer Satisfaction** Rating for U.S. LNPA services in 2012 (Proposal Section 2.5)
Factor 2: Vendor Experience and Performance	• History of serving of successfully providing Industry-wide, neutral third-party services for the Communications Industry and Government (Proposal Sections 2.1—Corporate Capabilities Table by evaluation criteria) • **Unmatched breadth and depth of experience** designing, developing, implementing/deploying, operating, and maintaining a LNP Administration Service and Systems **UNIQUE to the United States** in terms of stakeholders, types of portability, SLRs, Services required, neutrality requirements, transaction types and volumes, etc… (Proposal Section 2.4) • Unmatched experience in designing, implementing, and operating within a strict, audited neutrality environment—**no neutrality cure required** (Proposal Sections 2.3) • LNPA team **has over 420 years of direct LNP experience** (Proposal Sections 1.1, 1.2, 1.3, and 2.4)
Factor 3: Financial Stability	• LNPA contract is material to our business, and as a public company, provides rare financial and operation reporting and insight (Proposal Section 2.2) • Large enough to offer stability and reliability; small enough that the LNPA service remains primary focus of company (Proposal Section 2.2) • Not controlled by any foreign entities; operates LNPA contract within the United States (Proposal Section 2.2) • U.S. company respecting and adhering to U.S. laws and regulations (Proposal Section 2.2)
[redacted]	
	• [redacted] • **Fixed price with 100% cost certainty** • **Effective per transaction rate reduction of** [redacted] • **Increase in SLR/GEP penalties** • **Increase in Performance bonds commitments** • **Millions in savings from simplified, reduced, and eliminated "Direct Charges"** • **Avoids over $1.6 billion in unplanned and unbudgeted expense related to Industry transition**

Note: In submitting this response to the FoNPAC's BAFO survey, Neustar acknowledges and agrees to all of the terms and conditions set forth in all of the RFP surveys, including the RFP Survey, VQS, TRD Survey, and this BAFO Survey to the same extent that it did in its April 5, 2013 response, unless otherwise stated in this response. In its February 20, 2013 answer to Question #3, submitted on February 19, 2013 through the IASTA tool, the FoNPAC indicated that failure to agree with one or more of the terms and conditions does not disqualify a vendor from consideration. There has been no further communications with Respondents that supersedes this guidance.

Appendix B: RFP Pricing Compliance Table

The following corresponds to the Compliance Table from RFP Section 14.2. The Direct Charges from our April 5th submission have not changed.

Allocable Charges Compliance Table (in millions)

	Year 2015-2016	Year 2016-2017	Year 2017-2018	Year 2018-2019	Year 2019-2020	Year 2020-2021	Year 2021-2022
Allocable Industry Flat Fee in U.S. Dollars for All Combined NPAC Regions	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Allocable Industry Flat Fee in U.S. Dollars for MidAtlantic NPAC Region	NA	NA	NA	NA	NA	NA	NA
Allocable Industry Flat Fee in U.S. Dollars for MidWest NPAC Region	NA	NA	NA	NA	NA	NA	NA
Allocable Industry Flat Fee in U.S. Dollars for NorthEast NPAC Region	NA	NA	NA	NA	NA	NA	NA
Allocable Industry Flat Fee in U.S. Dollars for SouthEast NPAC Region	NA	NA	NA	NA	NA	NA	NA
Allocable Industry Flat Fee in U.S. Dollars for SouthWest Region	NA	NA	NA	NA	NA	NA	NA
Allocable Industry Flat Fee in U.S. Dollars for West Coast NPAC Region	NA	NA	NA	NA	NA	NA	NA
Allocable Industry Flat Fee in U.S. Dollars for Western NPAC Region	NA	NA	NA	NA	NA	NA	NA
Optional Regional Combination (must identify Regions)	NA	NA	NA	NA	NA	NA	NA

2.4 Best and Final Offer for Regional Fixed Rate Pricing—Option A

Based on our assessment that multiple LNPA Administrators creates unnecessary operational burdens for Service Providers and untenable risks to consumers, Neustar stands by its proposal to deliver a full, nationwide solution for U.S. LNPA Services. The primary expectation from service-intensive platforms like the NPAC/SMS is to create broad-based consistency and stability across a diverse group of stakeholders to ensure a uniform operating environment. The more deeply interconnected the service, the greater the ripple effect from non-uniform behavior, performance, and evolution. Solutions that enable common access to a single namespace (e.g. LERG, NANPA, Pooling, .org, etc.) operate with only a single vendor. In cases such as these, history shows that competition is best achieved via a process that selects the most effective full solution from competing offers, rather than via an inefficient segmentation of the solution itself.

In the case of the NPAC/SMS, a key contributor to the U.S.'s position delivering the world's most sophisticated and efficient LNP experience has been the benefit of a single, nationwide solution. Given the communications industry's overall evolution toward ever-increasing mobility and personalization, imposing artificial geographical barriers between Service Provider markets and consumers is certain to have unpredictable and costly impacts. While the technical specifications for the NPAC/SMS would theoretically be identical across multiple Administrators, the inevitable practical differences between highly complex solutions offered by multiple vendors would be certain to trigger additional costs to the many platforms and personnel currently interacting with the NPAC. These practical differences between vendors include, but are not limited to, software design, operational performance, service availability, customer support, regulatory governance, audits and controls, help desk practices, billing and collections, change management, staff experience, and more. These impacts will ultimately be felt by subscribers, affecting competition in the market and reducing consumer confidence.

The reasons the Industry should not consider solutions that involve two or more LNPA Administrators include, but are not limited to, the following:

- **The technology costs and risks of a regional NPAC/SMS transition are virtually identical to, if not higher than, those of a national NPAC/SMS transition.** Approximately 70% of telephone numbers in the NPAC/SMS are associated with Service Providers with a presence in more than one NPAC region. This implies that the vast majority of Service Providers currently connected to the NPAC/SMS would need to convert their SOA and LSMS platforms to support multiple LNPA Administrators, even if only a proportionally smaller area were selected for the transition.

- **Ongoing interactions with multiple LNPAs will result in additional operating costs to Service Providers who depend on and interact with the LNPA service.** Network transaction requests, platform maintenance and availability, reports and bulk data downloads, Service Provider configuration changes, vendor certifications, failover testing, and more would require duplicate interactions and overhead; costs of accommodating differences between the multiple vendors' procedures (for example, scheduling network migration projects across regions and Administrators) would be borne by the Service Provider.

- **The Industry as a whole would need to absorb the additional costs of managing two or more regional LNPA Administrators.** Determinations for the interactions between the vendors for NPAC.com, administration of

the LEAP and WDNC services, change management administration, and other common functions would have to be made by the Industry prior to implementation of a multi-Administrator environment and on an ongoing basis. The Industry may need to incur additional costs of a third party to ensure the two vendors are managed to the same level of consistency and quality achieved by Neustar today.

- **NPAC/SMS Innovation would be at the pace of the least-capable LNP Administrator.** Change management of the LNPA service and NPAC/SMS platform, with multiple Administrators, would engender longer and more costly debates over design and implementation schedules, given that all NPAC regions would require the exact same functionality to be implemented by the same time by different companies. Implementation schedules, performance expectations, and Service Provider integration requirements would be hampered by the lowest common denominator, since an outcome where one region received a higher quality experience than another would not be permitted by an industry used to receiving a uniform experience nationally. In an environment of rapid change, this would slow the Industry's ability to respond to FCC or market requirements, as compared to an environment with a single, highly capable LNP Administrator with responsibility for the whole country.

- **Multiple LNPAs inevitably means varying consumer experience in different parts of the country.** Studies have shown that the ease of number portability has a material effect on market competition and consumer confidence. Introducing multiple LNP Administrators at this time introduces the likelihood that consumers in the area of the country assigned to a less experienced Administrator would experience longer port times and more errors when porting their telephone numbers. This non-uniform experience will alter the competitive landscape in unpredictable ways, and is likely to lead to greater complaints to regulatory bodies. *See* Idaho Public Utilities Commission Comments at 3, September 12, 2013 (WC Docket Nos. 95-116, 07-149, 09-109) (stating that "[i]t is possible that seamlessness in number porting could be compromised with multiple vendors" . . . and "[t]his could result in less efficient service levels for customers in one region compared to the service provided by another vendor in a separate region").

- **The future of telephone number administration and addressing is likely to be one where numbers are fully independent of geography—a concept that runs contrary to establishing regional NPAC boundaries.** In a mobile and IP-based world, network addressing and routing no longer rely heavily on legacy geographic boundaries such as rate centers and LATAs. In times of emergency and disaster recovery, the NPAC/SMS's geographic restrictions have been temporarily removed, to allow for the porting of telephone numbers outside fixed artificial borders. In the future, this exception is likely to become the norm, as consumers take their phone numbers not just between Service Providers, but across the country as well. A segmentation of the NANP along geographic boundaries for LNPA purposes, in an environment where other geographic boundaries are being diminished and removed from the network, will again have unpredictable consequences for the consumer experience, network evolution, and support of the NANP for emerging business priorities such as machine-to-machine, just-in-time pooling, and least cost routing.

By selecting Neustar as the national U.S. LNP Administrator, the Industry and consumers will receive the benefits of continued performance, innovation, and neutrality nationwide, without any transition risk and without subjecting Service Providers and consumers to negative and expensive consequences. By contrast, a regional solution is too ill-defined and presents too many potential concerns to be a viable option for the U.S.

2.6 Best and Final Offer for Protection of Privacy

Neustar is the only Bidder that has demonstrated the efficacy of the security, privacy, and neutrality safeguards necessary today to ensure the continued integrity, confidentiality, and security of NPAC data.

There are many ways that NPAC data can be compromised. Security-Related Information

Security-Related Information

Further, it is important to note that, while at present, the NPAC/SMS doesn't contain any CPNI data, Neustar's corporate-wide neutrality, privacy, and security policies are designed to protect the most sensitive consumer data—which should both give the Industry confidence in our policies specific to LNPA AND provide comfort if and when additional data is entrusted to the LNPA and added to the NPAC/SMS per industry decisions in the future.

Our Standards, Policies, and Measures to Mitigate These Risks

Neustar uses the ISO 27001 standard for our information security framework and "Privacy by Design" for our privacy framework. ISO 27001 specifies an information security management system with explicit management controls. The standard contains 11 elements including security policy, asset management, access control, and compliance. The principle of Privacy by Design takes personal privacy into consideration throughout the process of designing, building, and delivering information products and services.

Table 2.6-1 Neustar Neutrality, Security, and Privacy Documents

Document	Description
[redacted]	[redacted]
Information Security Policy	• Establishes rules and procedures for protecting Neustar's confidential information as well as the software, hardware, and other equipment or technology used to access, collect, generate, process and/or store that information. • Governs use of Personal Devices, third party equipment, or other technology to access Neustar's Information and IT Resources. • Applicable to all personnel (including contractors), systems, and business areas. • Senior leadership throughout Neustar have reviewed and approved this Policy, and employees at all levels are accountable for ensuring compliance with its requirements.
Security Related Information [redacted]	[redacted]
Privacy Principles	• Articulates the company's commitment to "privacy by design" framework. • Sets forth the principles governing our collection, use, storage, and disclosure of information that can be used to identify individuals.
[redacted]	[redacted]
Records Management Policy	• This Policy, together with the Records Retention Schedule, describes the policies, practices, and procedures to be followed to ensure Neustar fully complies with all applicable laws, regulations, and best professional practices. • Sets out the policies and procedures to be followed by all employees and authorized third parties to ensure Neustar records are: o managed in a consistent, systematic, and reliable manner; o available when required for legal, regulatory or operational reasons; and o discarded in an orderly manner when no longer needed.

Table 2.6-1 Neustar Neutrality, Security, and Privacy Documents

Document	Description
[redacted]	[redacted]
	Security-Related Information
Neustar Policy on the Acceptable Use of Technology Resources	• Sets forth the policies and procedures governing use of Neustar information technology resources. • Reflects Neustar's policy limiting access to Confidential Information to authorized staff with a need to know for legitimate business purposes. • Imposes personal responsibility for each user to comply with law, regulation, and Neustar policy. • Establishes that users may have no expectation of privacy with respect to use of Neustar IT Resources and information created or stored on such resources and sets out Neustar's monitoring and access rights. • Describes user obligations with respect to information security including access, encryption, incident reporting, remote access, mobile computing, etc.

NEUSTAR CODE OF CONDUCT

1. Neustar will never, directly or indirectly, show any preference or provide any special consideration to any company that is a telecommunications service provider, which term as used herein shall have the meaning set forth in the Telecommunications Act of 1996.

2. No shareholder of Neustar shall have access to user data or proprietary information of the telecommunications service providers served by Neustar (other than access of employee-shareholders of Neustar that is incident to the performance of NANPA and LNPA duties).

3. Shareholders of Neustar will ensure that no user data or proprietary information from any telecommunications service provider is disclosed to Neustar (other than the sharing of data incident to the performance of NANPA and LNPA duties).

4. Confidential information about Neustar's business services and operations will not be shared with employees of any telecommunications service provider. Neustar shareholders will guard their knowledge and information about Neustar's operations as they would their own proprietary information.

5. No person employed by, or serving in the management of any shareholder of Neustar will be directly involved in the day-to-day operations of Neustar. No employees of any company that is a telecommunications service provider will be simultaneously employed (full-time or part-time) by Neustar.

6. Warburg Pincus will not control more than 40% of Neustar's Board.

7. No member of Neustar's board will simultaneously serve on the board of a telecommunications services provider.

8. No employee of Neustar will hold any interest, financial or otherwise, in any company that would violate the neutrality requirements of the FCC or the NPAC Contractor Services Agreements (the Master Agreements).

9. Neustar will hire an independent party to conduct a neutrality review of Neustar, ensuring that Neustar and its shareholders comply with all the provisions of this Code of Conduct. The neutrality analyst will be mutually agreed upon by Neustar, the FCC, NANC and the LLCs. The neutrality review will be conducted quarterly. Neustar will pay the expenses of conducting the review. Neustar will provide the analyst with reasonable access to information and records necessary to complete the review. The results of the review will be provided to the LLCs, to the North American Numbering Council and to the FCC and shall be deemed to be confidential and proprietary information of Neustar and its shareholders.

Implementing these policies and practices for the NPAC requires interpreting the documents and a detailed knowledge of number portability and the needs of the user community. Some NPAC-specific measures we have implemented are highlighted in Table 2.6-2.

2.6-2 NPAC-Specific Measures to Ensure Security and Privacy of Data

Component	Description and Measures
[redacted]	[redacted]
Neustar Corporate Neutrality Audits	Third-party auditors: • Review all certifications of each employee, board member, officer, certifying their adherence with the neutrality compliance program including: o the protection of the confidential and proprietary data of Neustar and its customers, o the prohibition on being simultaneously employed by Neustar and a telecommunications service provider (TSP) or interconnect VoIP provider, or o the prohibition on owning five percent or more of a TSP. • Examine Neustar ownership to ensure no TSP or interconnected VoIP provider owns 5% or more equity or voting interest in the company. • Verify on a quarterly basis that Neustar has not derived a majority of its revenue from, or issued a majority of its debt to, any single TSP. • **Results—100% Compliance Over the Last 5 Years**
[redacted]	[redacted]

2.6-2 NPAC-Specific Measures to Ensure Security and Privacy of Data

Component	Description and Measures
Security Training and Certifications	• Neustar provides Security awareness training to all employees—upon hire and yearly thereafter. Security-Related Information • **Results: 100% Compliance**
NPAC/SMS Data Center Operations Audit (Article 14 Audit)	• An independent, intensive third-party review of Neustar's NPAC data center and operations has found that these areas have consistently exceeded or far exceeded industry best practices in all tested areas year-over-year, including both Business Continuity Management and Security. • **Results: Exceeding or Far Exceeding industry best practices over the last 5 years. See following Exhibit for Security-specific portion of the audit).**

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

2.6-2 NPAC-Specific Measures to Ensure Security and Privacy of Data

Component	Description and Measures
NUE Process and NUE Audit	Third-party auditors ensure Neustar, in its activities as a User, is not advantaged because it is also the LNPA. The auditors: • Review **every use** of User Data by Neustar's User Services, and determine whether access to the NPAC is necessary and the intended use is a Permitted Use. All other providers of telecommunications-related services are reviewed only for their initial proposed use of User Data. • Validate, annually, with the Director of Customer Experience and Director of Operations that Neustar's LSMS receives the same data as all other Users. o A sample Subscription Version transaction is selected from each NPAC Region production database, and is then compared to the sample Subscription Version transaction record in the NPAC Region bulk data download (BDD) file that is generated for the Neustar LSMS. • **Results: 100% compliance since inception in 2009.**
[redacted]	Security-Related Information

Security–Article 14 Audit Scores

Category	2009	2012	Trend
Security Overall Score	**4.50**	**4.50**	⟷
Security Governance	**4.30**	**4.37**	▲
Security Policy	4.30	4.50	▲
Security Awareness Training	4.40	4.40	⟷
Security Compliance	4.20	4.20	⟷
Firewall	Security-Related Information		⟷
Remote Access			⟷
Network Security			⟷
Host Systems & Database Security			⟷
Data Center Security			⟷

5 - Excellent performance, far exceeds industry best practices
4 - Above average performance, generally exceeds industry best practices
3 - Average performance, meets industry best practices
2 - Below average performance, fails to meet industry best practices
1 - Poor performance, falls far below industry best practices

Neustar Acceptable Use of Technology Resources Policy

Version 2.2

Effective Date: September 3, 2013

neustar™

Table of Contents

1 Purpose and Goals

Neustar, Inc. ("Neustar") relies on information technology resources as an essential part of the company's day-to-day business activities. These resources are intended for use by employees and others in support of Neustar's goals and objectives. You must use company technology only in compliance with applicable law and Neustar policies designed to protect confidential and proprietary information belonging to Neustar and/or our clients and avoid compromise of Neustar IT resources, information and data. This policy, along with referenced policies, sub-policies, standards, and procedures (collectively, this "Policy") sets out the policies and procedures governing your use of Neustar information technology resources (as defined below, "IT Resources").

2 Scope

This Policy applies to all individuals using Neustar IT Resources to collect, access, create, use, store or otherwise process information, wherever located, and whether through direct or remote access to Neustar's technology. This Policy also applies to individuals using Personal Devices, as defined in the Neustar Personal Device User Policy and Agreement to access Neustar IT Resources or company information (as defined below, "Confidential Information"). Individuals covered by this Policy, include, without limitation:

- Full and part-time Neustar employees;
- Contract and temporary personnel, including consultants on temporary engagement;
- Clients, customers, vendors, service providers, business partners and any other party that has access to Neustar IT Resources; and
- Neustar visitors and guests.

The Policy governs your use of all Neustar IT Resources including computers, printers, copiers, faxes, mobile devices, removable media (thumb drives, CDs, external USB hard drives, tape drives etc.), and Neustar networks, including the virtual private network ("VPN") and web portal, electronic communication channels such as email or web mail, mobile and fixed telephones, voicemail, and access to any public services such as the Internet.

This Policy applies to your use of Personal Devices, third party equipment, or other technology to access Neustar's Confidential Information and/or IT Resources.

This Policy applies to both your business and personal use of IT Resources. Although Neustar permits limited personal use of IT Resources, as described in this Policy, you may not use Confidential Information except on behalf of Neustar, in furtherance of its goals and objectives, and as required to perform your job function.

3 Definitions

Confidential Information includes all of Neustar's proprietary business information, including, without limitation, the following:

- Information relating to Neustar's planned or existing computer systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods;
- Information regarding existing, former, or prospective Neustar customers, and any information received from such customers or created by Neustar in the course of providing services ("Customer Information");

- Information that identifies or can be used to identify specific individuals including Neustar employees and/or their dependants and beneficiaries, applicants for employment, customers and their subscribers or end users, and others ("Personal Information");
- "Sensitive Personal Information" is a subset of Personal Information consisting of a person's name in combination with an item such as (1) a social security number or other government-issued identifier; (2) a credit card, bank account, or other financial account number; (4) medical, lifestyle, or other highly personal information;
- Business information relating to Neustar and its affiliates including financial information, organizational structure, business initiatives, intellectual property, product plans, design or requirements documents, and strategic or other plans;
- Confidential information of third parties, including Neustar's customers, vendors, suppliers, contractors, partners, and acquisition targets;
- Other confidential and/or proprietary information that Neustar receives, uses, creates, stores, and/or transmits as part of its day-to-day business activities; and
- Any information that someone familiar with Neustar's business would consider confidential or proprietary, the maintenance of which would be important to Neustar, its employees, and/or its customers.

An ***Electronic Communication*** is the transmission of Electronic Information via an Electronic Communication Channel.

An ***Electronic Communication Channel*** is any service supporting communication and collaboration between users such as Email, Instant Messaging, participation in shared sites, and Internet communication and collaboration services (including online social media services).

Electronic Information is any information artifact created, stored, transmitted, or accessed using IT Resources, Personal Devices, or other technology that is used to access, collect, create, process and/or store Neustar's Confidential Information. This includes electronic documents, emails, instant messages, voicemails, activity logs and records, and data in Neustar data stores.

Neustar Equipment is any physical device made available to you by Neustar. This includes laptops, notebooks, desktops, Blackberries, Smart phones, tablets, copiers, faxes, telephones, Neustar-issued personal communication devices, and printers.

The ***Neustar Network*** is the hardware and software electronically connecting Neustar hardware and software and providing access to the Neustar Intranet, Neustar web-based applications and data, and the public Internet.

Neustar IT Resources include the Neustar Network, Neustar Equipment, and all hardware and software components of Neustar's information technology including computers, printers, copiers, faxes, mobile devices, removable media (thumb drives, CDs, external USB hard drives, tape drives etc.), and Neustar networks, including the virtual private network ("VPN") and web portal, electronic communication channels such as email or web mail, mobile and fixed telephones, voicemail, and access to any public services such as the Internet.

Legitimate Business Purposes for reviewing documents, communications (including Electronic Communications), or other information created, stored, or transmitted using

Neustar IT Resources or Personal Devices include, but are not limited to the following situations:

- Routine monitoring for quality control and to ensure proper operation of Neustar systems, to verify specific transactions, and to audit compliance with law, regulation, and/or Neustar's policies, including without limitation, its policies on information security, discrimination, harassment, use of trade secrets, and securities-related information;
- Internal or external investigations to determine if there have been violations of Neustar's workplace policies or criminal or civil wrongdoing; and
- Access to Confidential Information under your control at any time that you are unavailable and there is a business need to review that information on an expedited basis.

NeuCIRT (Neustar Cyber Incident Response Team) was formed in 2012 and is dedicated to protecting Neustar and its customers' networks and data through intelligence gathering, security monitoring, threat detection, incident response, and digital forensics. NeuCIRT can be contacted via email at Neucirt@neustar.biz or by phone at 1-855-NEUCIRT (1-855-638-2478)

A ***Personal Device*** is any personally-owned computing or electronic storage device including desktop PCs, laptops, smartphones, tablet computers, or any future developed device that that you use to connect to the Neustar IT Resources or to access Confidential Information.

Personal Information is any information that can be used, alone or in combination with other readily available information, to identify a specific individual.

Portable Storage Media is any portable device on which Electronic Information can be stored, including laptops, notebooks, tablets, PDA's, thumb drives, iPods, external USB drives, and digital cameras.

4 General Use, Ownership, and Privacy

4.1 Personal Responsibility

You are personally responsible for familiarizing yourself and complying with this Policy, and for maintaining the confidentiality and integrity of Confidential Information and IT Resources.

4.2 Compliance with Law and Regulation

You must not use Neustar IT Resources in a manner that violates Neustar policy or applicable laws and regulations. Consult your supervisor, manager, or business contact if you have any questions about a policy, its applicability, or the procedures you should follow in order to adhere to the policy.

4.3 Ownership

Confidential Information and any Electronic Information and Communications created, received, sent or stored using Neustar IT Resources is assumed to have been created on behalf of Neustar, in furtherance of its goals and objectives, and is considered company property.

4.4 Access and Monitoring

To the extent permitted by applicable law and undertaken for a Legitimate Business Purpose, Neustar reserves the right to block access to, audit, monitor, access, record, and disclose any Electronic Information and/or Electronic Communications, whether or not it contains Confidential Information created, received, sent, or stored on Neustar IT Resources and/or Personal Devices.

4.5 No Expectation of Privacy

You may have no expectation of privacy for any information, including Electronic Information or Electronic Communications created, stored, used or transmitted using Neustar IT Resources. Your expectation of privacy with respect to information residing on Personal Devices used to access Confidential Information and/or IT Resources is limited in accordance with the Personal Device User Policy and Agreement.

4.6 Data Privacy

Neustar uses data to help businesses serve their customers, deliver personalized content, and prevent fraud without sacrificing personal privacy. These Privacy Principles govern our collection, use, storage, and disclosure of information that identifies or can reasonably be used to identify a specific person. All employees are required to adhere to the Neustar Privacy Principles.

4.7 Consent

Your use of Neustar IT Resources constitutes your consent to Neustar's access to, and review, monitoring and/or recording of Electronic Information or Electronic Communications for a Legitimate Business Purpose.

5 Records Management

Confidential Information created, stored, used or transmitted using Neustar IT Resources and/or Personal Devices used to access Confidential Information or IT Resources is subject to Neustar's Records Management, Retention, and Disposal Policy, the Retention Schedules, and Classification Matrix.

6 Respect for Intellectual Property

Neustar respects the intellectual property rights of Neustar and third parties, and prohibits use of Neustar IT Resources in a manner that infringes rights arising under copyright, trademark, patent, or trade secret law. Contact the General Counsel if you have any questions about intellectual property.

7 Personal Use of Neustar IT Resources

7.1 Personal Use

Neustar permits limited, incidental, and non-commercial use of Neustar IT Resources provided that it does not involve the use of Confidential Information or interfere with your regular duties and responsibilities.

7.2 Labeling and Segregation

Segregate and clearly label all personal information or communications that you store on Neustar IT Resources (i.e., by creating "Personal" email and document folders).